UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/725,910	11/30/2000	Chenggang Duan	3731-0141P	9772

30595 7590 01/07/2005

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/725,910	DUAN ET AL.	
	Examiner	Art Unit	
	Matthew T Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08/16/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 08/16/2004.

Begin FAOM Dated 5/13/2004

1. Claims 1-26 have been examined.

Title

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

3. The following title is suggested: *Combining One-Time Pad Data Encryption and Adaptive Text Compression*

Priority

4. This application claims foreign priority, under Title 35 U.S.C. 119 (a-d), to Chinese Application 00134266.5.

Acknowledgment is made of applicant's claim for foreign priority based on an application filed in China on November 29, 2000. It is noted, however, that applicant has not filed a certified copy of the 00134266.5 application as required by 35 U.S.C. 119(b).

The effective filing date of the subject matter defined in the pending claims of this application is 11/30/2000.

Information Disclosure Statement

5. The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information

submitted for consideration by the Office, and MPEP § 609 A(1) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the examiner, on form PTO-892, has cited the references, they have not been considered.

Drawings

6. The drawings filed on January 3, 2002 are objected to because:

Figure 1 should be designated by a legend such as –Prior Art—because only that which is old is illustrated. See MPEP § 608.02(g).

Figures 3 and 7 are inconsistent with the specification because Figure 7 is an encryption flow diagram and Figure 3 is a decryption flow diagram.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

7. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: 132 and 134. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

8. The abstract of the disclosure is objected to because the statement "decryption device and method progress encrypted text" does not make sense because "method progress encrypted" is

not grammatically correct and therefore must be corrected. Correction is required. See MPEP § 608.01(b).

9. The disclosure is objected to because of the following informalities:

Page 8 Paragraph 3 refers to frequency table 130 of figure 4. However, element 130 of figure 4 is not consistent the frequency table, which is illustrated as RAM's 126.

Appropriate correction is required.

Claims

10. The applicant is reminded that a series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

Claim Objections

11. Claims 1-26 objected to because of the following informalities:

Claims 1, 5-6, 8-9, 11, 14-15, 19-20, 22-23, 25 all recite "the at least one", "the at least two", or "a different at least one". These phrases are not grammatically correct and must be

changed. The examiner suggests changing both "the at least one" and "the at least two" to "said". Appropriate correction is required.

Any claim not specifically addressed above is objected to by virtue of its dependency.

Claim Rejections – 35 USC § 112

12. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> *The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.*

13. Claims 15-19, 21-22 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claim 15 claims a decoder that produces plain text. However, claim 15 never discloses the decoder receiving encoded text. It is inherent that the decoder receives encoded text in order for it to decode. Therefore, this claim is not enabling.

Claims 16-19, 21-22 are rejected by virtue of their dependency on claim 15 and because they do not provide the necessary encoded text to make the claim enabling.

For purposes of searching art, based on Figure 8 of the disclosure, the examiner will assume the decoder receives cipher text and not plain text.

14. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

15. Claims 10, 15-22, and 24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

16. Claim 10 Line 2 and claim 24 line 2 recite "of a length equal to a key." This statement fails to particularly point out the scope of the claim. This is because the ordinary person skilled in the art would be unable to determine what length is equal to the length of a key.

17. Claim 20 claims dependency to the decryption device of claim 1. However, claim 1 does not disclose a decryption device, but rather an encryption device. Therefore the scope of this claim is unclear because the ordinary person skilled in the art could not determine weather this claim depends on an encryption device or a decryption device. The examiner will assume, for purposes of searching prior art, that claim 20 is dependant on the decryption device of claim 15.

18. Claim 21 recites the limitation "said encoder" in lines 1-2. There is insufficient antecedent basis for this limitation in the claim. Therefore, the scope of the claim is unclear because one of ordinary skill in the art would not be able to determine if the device is encrypting or if it is decrypting. The examiner will assume, for the purpose of searching art, that the phrase "ciphered text output by said encoder is based" was meant to be "plain text output by said decoder is based".

19. Claim 15 Line 2 recites "and plain text" and Line 4 recites "outputting plain text". These two recitations of "plain text" render the scope of the claim unclear because one of ordinary skill in the art would be unable to determine if the two "plain texts" are the same plain text.

Claim 15 Lines 4-6 recite "the plain text". The ordinary person skilled in the art would be unable to determine which plain text is being referred to by "the plain text". Therefore the scope of the claim is unclear.

20. Claims 16-22 are rejected by virtue of their dependency to claim 15.

Claim Rejections – 35 USC § 102

21. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> *A person shall be entitled to a patent unless –*
>
> *(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.*

22. Claims 1-5, 7-20, 21-26 rejected under 35 U.S.C. 102(b) as being anticipated by Witten et al. (*On the Privacy Afforded by Adaptive Text Compression*) hereinafter referred to as Witten.

23. Regarding claim 1, Witten disclosed an adaptive text compression technique, which uses an adaptive model and an encoder (See Witten Section 2). Witten also disclosed a random number generator taking a secure seed and producing a key for the model (See Witten Page 405 Col. 1 Paragraph 1). Witten disclosed that the model produced symbol counts to determine the probability of a symbol occurring (See Witten Section 5).

24. Regarding claim 2, Witten disclosed the key size depending on the alphabet being encoded (See Witten Page 405 Paragraph 1).

25. Regarding claim 3, Witten disclosed the output varying depending on the input (See Witten Section 4).

26. Regarding claim 4, Witten disclosed a seed and a random number, which are used as the two keys (See Witten Page 405 Paragraph 1).

27. Regarding claim 5, Witten disclosed a table maintaining frequency counts (See Witten Section 5 Paragraph 4).

28. Regarding claim 7, Witten disclosed the possibility of choosing the alphabet to be the binary alphabet (See Witten Section 10 Paragraph 3).

29. Regarding claim 8, Witten disclosed the random key being used as the initial frequency table of the model (See Witten Page 405 Paragraph 1).

30. Regarding claim 9, Witten disclosed using a seed and a random number to create a frequency table (See Witten Page 405 Paragraph 1) and using the frequency table to encode plain text (See Witten Section 3).

31. Regarding claim 10, Witten disclosed creating a random key (See Witten Page 405 Paragraph 1). It was inherent that the key was as long as a key, because if it was not as long as a key, it could not be used to properly initialize the frequency table.

32. Regarding claim 11, Witten disclosed that the key is used as the initial frequency table (See Witten Page 405 Paragraph 1). Therefore, it is inherent that different keys will produce different frequency tables.

33. Regarding claim 12, Witten disclosed the output varying depending on the input (See Witten Section 4).

34. Regarding claim 13, Witten disclosed the possibility of choosing the alphabet to be the binary alphabet (See Witten Section 10 Paragraph 3).

35. Regarding claim 14, Witten disclosed the random key being used as the initial frequency table of the model (See Witten Page 405 Paragraph 1).

36. Regarding claim 15, Witten disclosed an adaptive text de-compression technique, which uses an adaptive model and a decoder (See Witten Section 2). Witten also disclosed a random number generator taking a secure seed and producing a key for the initial model (See Witten Page 405 Col. 1 Paragraph 1). Witten further disclosed encoding the initial model, and sending it to the decoder (See Witten Page 405 Col. 1 Paragraph 1). Witten disclosed that the model produced symbol counts to determine the probability of a symbol occurring based on the decoded plain text (See Witten Section 5).

37. Regarding claim 16, Witten disclosed the key size depending on the alphabet being encoded (See Witten Page 405 Paragraph 1).

38. Regarding claim 17, Witten depicts the output of the decoder being the same as the input to the encoder (See Witten Figure 2). Therefore as the input to the encoder varies, the output of the decoder must vary as well.

39. Regarding claim 18, Witten disclosed a seed and a random number, which are used as the two keys (See Witten Page 405 Paragraph 1).

40. Regarding claim 19, Witten disclosed a table maintaining frequency counts (See Witten Section 5 Paragraph 4).

41. Regarding claim 21, Witten disclosed the possibility of choosing the alphabet to be the binary alphabet (See Witten Section 10 Paragraph 3).

42. Regarding claim 22, Witten disclosed the random key being used as the initial frequency table of the model (See Witten Page 405 Paragraph 1).

43. Regarding claim 23, Witten disclosed using a seed and a random number to create a frequency table (See Witten Page 405 Paragraph 1) and using the frequency table to decode cipher text (See Witten Figure 2 and Section 3).

44. Regarding claim 24, Witten disclosed creating a random key (See Witten Page 405 Paragraph 1). It was inherent that the key was as long as a key, because if it was not as long as a key, it could not be used to properly initialize the frequency table.

45. Regarding claim 25, Witten disclosed that the key is used as the initial frequency table (See Witten Page 405 Paragraph 1). Therefore, it is inherent that different keys will produce different frequency tables.

46. Regarding claim 26, Witten depicts the output of the decoder being the same as the input to the encoder (See Witten Figure 2). Therefore as the input to the encoder varies, the output of the decoder must vary as well.

Claim Rejections – 35 USC § 103

47. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

48. Claims 6 and 20 rejected under 35 U.S.C. 103(a) as being unpatentable over Witten as applied to claims 1 and 15 respectively above, and further in view of examiner's official notice.

Witten disclosed storing the model in memory and updating the model throughout the encoding and decoding process (See Witten Section 8). However, Witten failed to disclose the memory being Random Access Memory (RAM).

The examiner takes official notice that it is well known in the art to use RAM to store data that is being read and written on a regular basis.

It would have been obvious to the ordinary person skilled in the art at the time of the invention to employ RAM as the memory in the encoder and decoder of Witten. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the table to be updated throughout the encoding and decoding process.

Conclusion

49. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Witten et al. (*Arithmetic Coding for Data Compression)* disclosed a method of data compression using a fixed-model.

b. Bergen et al. (*Data Security in a Fixed-Model Arithmetic Coding Compression Algorithm*) disclosed the flaws of the fixed-model arithmetic coding technique of Witten et al.

c. Vernam (U.S. Patent Number 1,310,719) disclosed a one-time pad encoding apparatus.

d. Chamzas et al. (U.S. Patent Number 4,973,961) disclosed an arithmetic encoder.

e. Degele (U.S. Patent Number 5,297,207) disclosed a pseudo-random key generator.

f. Mischenko (U.S. Patent Number 6,301,361) disclosed a random key generator and encoder using the same.

END FAOM Dated 5/13/2004

---

50. All rejections and objections not set forth below have been withdrawn.

51. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file. Therefore, the effective filing date of this application is 11/29/2000.

Response to Arguments

52. Applicant's arguments filed 08/16/2004 have been fully considered but they are not persuasive. Therefore, the examiner maintains the rejections of claims 1-9, 11-23, and 25-26, as presented in the first action on the merits dated 5/13/2004.

53. Regarding the arguments to the rejection of claim 1, the applicant traverses primarily that **I**. A seed used to generate a random number is not a key, **II**. The random number generator of Witten does not receive a main key and generate a working key, and **III**. The model does not receive a main key and a working key.

I. The argument that a seed of a random generator is not a key is not persuasive because it provides no evidence to support the statement that a seed is not a key. In fact, because the seed affected the output of the random number generator, it acted as a key, which can be called a main key, for the random number generator (See Witten Page 405 Col. 1 Lines 8-12).

II. The argument that the random number generator does not take a main key and produce a working key is not persuasive. The random number generator of Witten received the seed, or main key, and produced the initial model, or working key (See Witten Page 405 Col. 1 Lines 1-12).

III. The argument that the model does not receive a main key and a working key is not persuasive. Witten disclosed that the initial model, or working key, was generated by the random number generator (See Witten Page 405 Col. 1 Lines 1-12), which implies that it was then received by the model in order to have initialized model. Witten also disclosed securely transmitting the seed, or main key, (See Witten Page 405 Col. 1 Lines 8-12), and

that the model receives all the transmitted data (See Witten Page 404, Col. 3 Paragraph 4), which suggests that the seed was provided to the model when it was securely transmitted.

54. Regarding the arguments to the rejection of claims 9 and 23, the applicant traverses primarily that Witten did not disclose processing key bits of a key to generate the frequency table, which is not persuasive. Witten disclosed using a seed, or main key, to produce an initial model in the form of random numbers (See Witten Page 405 Col. 1 Lines 1-12) which suggests that the bits of the seed, or main key, were processed by the random number generator in order to produce the random numbers. Witten also disclosed that the initial model was used as a key (See Witten Page 405 Col. 1 Lines 4) and that the key depended upon all the previously transmitted text (See Witten Page 404 Col. 3 Paragraph 4). Witten further disclosed that the frequencies were derived from the initial model, or working key, which was dependant upon the processing of the seed, or main key, bits (See Witten Page 405 Col. 1 Lines 12-21).

55. Regarding the arguments to the rejection of claim 15, the applicant traverses primarily that **I**. The model does not receive a main key and a working key, and **II**. The random number generator did not receive plain text from the model.

I. The argument that the model did not receive a main key and a working key is not persuasive. As discussed above with regards to claim 1, Witten suggested that the seed, or main key, was sent through the model and encoder to the receiver (See Witten Page 405 Col. 1 Lines 1-12). Witten also disclosed that the model at the receiver represented the changing symbol frequencies seen so far in the message, and that the transmitter and receiver must both use the same initial value, or working key, in order for the models to

stay in sync and for decryption to be performed accurately (See Witten Page 402 Col. 2 Paragraph 3). This suggests that both the seed, or main key, and the initial model, or working key, must have been received by the model at the receiver in order for the models to have been synchronized.

II. The argument that the random number generator did not receive plain text is also not persuasive. In order for the securely transmitted seed, or main key, to have been used in the random number generator of the receiver as is implied by the teachings of Witten (See Witten Page 405 Col. 1 Lines 1-12), it must have been decoded by the model and sent to the random number generator for producing the initial model, or working key.

56. Regarding the arguments to the rejection of claims 2 and 16, the applicant traverses primarily that the working key of Witten was not variable in length. Witten disclosed that the initial model, or working key, "need not be large – an array of single-character frequencies in the range of, for example, 1-10, one for each character in the alphabet, would do" (See Witten Page 405 Col. 1 Lines 1-8). Therefore, the size of the working key depended on the number of characters in the alphabet being encoded, and therefore was variable length.

57. Regarding the arguments to the rejection of claims 4 and 18, the applicant traverses primarily that that the seed of Witten was not a key ad therefore Witten did not disclose the different working and main keys. Simply because Witten did not call the "seed" a "key", does not mean it is not a key. The random number generated by the random number generator depended on the seed, which had to be transmitted in order for proper decryption, and therefore the seed was a key for the random number generator.

58. Regarding the arguments to the rejection of claims 7, 13, and 21, the applicant traverses primarily that processing a binary alphabet does not anticipate a bit-based processing scheme. Witten disclosed that the frequency was updated for each symbol, zero or one, and is therefore a bit-based processing scheme (See Witten Section 10 Paragraph 3).

Response to Amendment

59. The rejection of claims 10 and 24 above is withdrawn because the scopes of claims 10 and 24 have changed due to the amendment of the claims.

60. Claims 10 and 24 are rejected under 35 U.S.C. 102(b) as being anticipated by Witten as applied to claims 9 and 23 above respectively. Witten disclosed that the random number generator would generate the key (See Witten Page 405 Col. 1 Lines 1-12). Therefore, the random number generator must have generated a random number the length of the key.

Conclusion

61. Claims 1-26 have been rejected.

62. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

63. Please direct all inquiries concerning this communication to Matthew Henning whose telephone number is (571) 272-3790. The examiner can normally be reached Monday-Friday from 9am to 4pm, EST.

If attempts to reach examiner by telephone are unsuccessful, the examiner's acting supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The fax phone number for this group is (703) 305-3718.

Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Matthew Henning
Assistant Examiner
Art Unit 2131
1/3/05

EMMANUEL L. MOISE
PRIMARY EXAMINER